

Voice Over IP:

Voice-over-IP comes from the VoIP Forum, a development by major equipment providers such as Cisco, VocalTec, 3Com, and Netspeak to promote the use of ITU-T H.323, the standard approved by the International Telecommunication Union (ITU) in 1996 for sending voice information using the Internet Protocol,

Voice-over-Internet Protocol or more simply VoIP is a term used in telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). It is a technique that allows voice traffic to be transported across an IP-based data network or the Internet instead of on the traditional circuit-switched network. The voice signal is sampled, compressed and encapsulated into data packets to allow it to be switched, routed and bridged along with all other data packets across the Local and Wide area network.

When talking about VoIP there are two parts to the story: IP Trunking and IP Extensions. IP Trunking is where multi-site systems transport telephone calls over their wide area network. The phones at each end don't necessarily have to be IP phones. IP Trunking is used to tie the two systems together. Voice effectively travels for free over the existing data network.

IP Extensions, or IP in the LAN, is where the extensions are IP Data devices working off the LAN. They can be multimedia soft phones such as Net meeting, or alternatively IP telephones (IP Hard phone) which replicate a traditional telephone. As these technologies have emerged, many questions as well as common myths haven arisen regarding their deployment and operation. So here we are providing some facts, which will help you to take intelligent decisions about deploying converged network and IP communications solution.

Fundamental standards for IP based communication are already in place; new standards will continue to emerge:

In the world of technological revolution, it can take often less than a year for a standard to become obsolete. Most of the standards that are critical to the success of the IP communications have been around for some time. Lets start with the newest standard- inline power over Ethernet 802.3af was finalized by the institute of Electrical and Electronics engineers (IEEE) in early 2003. According to the standard, when the phone boots up ,it uses the Dynamic Host Configuration Protocol (DHCP) to obtain its IP address from the appropriate server, just like a PC does. The phone then downloads the operations system using Trivial File transfer protocol (TFTP)- again , just like many other network devices. Then, it sets up an 802.3p virtual local-area network (VLAN) to segregate the voice traffic for optimum quality of service (QoS) and security. With transport layer security (TLS) secure socket Layer and secure Real Time Protocol (SRTP). The signaling of communication call setup, and processing to and from Call Manager and other endpoints is protected and secure.

The next standard that comes into operation when the user takes the phone off the hook, causing the phone to send a message to the Call Manager call processing software using Session Initiation Protocol (SIP). Gateways devices talk to the call manager using H.23 or Media Gateway Control Protocol (MGCP). Most of the standards used to make a IP phone call are not new. As new protocols become standards, they can be easily added to the total IP communication and the investment you make today will be protected for years to come.

IP Communications solutions are proven to offer lower TCO and high:

The typical IP phone today costs the same or less than an equivalent digital desk phone set. When you factor in the lower overall total cost of ownership that results from an IP communications solution running on a converged IP network for voice , video and data , an IP communications solution can save organizations a substantial amount of money.

There are many applications today that cuts cost, increase productivity, and improve customer satisfaction:

The true power of IP communications lies in the convergence of voice, video and data applications for the user. The architecture of IP communications allows applications to be integrated with organization's existing applications, from existing e-mail, CRM , calendar systems to vertical applications such as inventory lookup, hotel wake-up calls and school attendance. Just like there is no single reason for the adoption of the internet, there is no single reason to adopt IP communications.

IP Communications solutions are secure and reliable:

Security is an important issue- whether or not you are running voice on your data network. But the real myth is that hybrid systems are more secure than end- to- end IP communications solutions.

Everyone is familiar with how a traditional digital PBX is put together. With these systems, you have to protect against toll fraud, masquerading and war dialing. And with traditional systems, unauthorized access or eavesdropping can often be accomplished with a simple pair of alligator clips; but, you probably don't have to worry about internet worms. However, some people think that you don't need to worry about network security if you opt for one of the hybrid migrations strategies being promoted by the traditional vendors.

Typically, the first step in hybrid migrations process is pulling CPU and call Processing out of the cabinet and putting it on a dedicated LAN. You must them make sure that LAN is completely secure, since an attack on the call processing component affects every user on the system- not just phone users. In this scenario, not only do you have the same security considerations as if the entire solution was on the IP network, but you also have to manage two separate networks, without realizing the benefits of having an integrated solution on a single, converged network.

When protecting against the types of vulnerabilities common to voice and voice related systems, it's important to focus on three critical components.

Privacy: Via secure connectivity. Technologies such as IP Security (IPSec) and SSL virtual private networks (VPN) help to ensure that communications over both the wide-area network (WAN) and LAN are secure.

Protection: Via threat defense systems. Technologies such as firewalling and intrusion prevention systems combat threats from both internal and external sources,

Control: Via trust and identify systems. Access control servers and the Cisco Network Admission control (NAC) program enable organizations to control access to information, letting the right people get the tight information at the right time.